IN THE CLAIMS:

Please amend claims 11-20 and add new claims 21-30 as shown below.

The pending claims are believed to be as follows:

Claims 1-10 (canceled).

11. (currently amended) ~~M~~A method of encryption and decryption carried out by ~~a plurality of~~ at least three encryption/decryption modules arranged in series, wherein ~~a~~ each intermediate and the last encryption/decryption module~~, different from the first module, starts~~ begins encryption/decryption operations ~~as soon as said module receives a part of the results of encryption/decryption operations from~~ before the immediately preceding encryption/decryption module has terminated its encryption/decryption operation, wherein at least one encryption/decryption module operates with a type of encryption/decryption algorithm using asymmetric keys including a private key and a public key.

12. (currently amended) ~~M~~A method according to Claim 11, wherein ~~a~~ each intermediate and the last decryption module~~, different from the first module, starts~~ begins decryption operations as soon as said module receives a part of the results of decryption operations from the immediately preceding decryption module.

13. (currently amended) ~~M~~A method according to Claim 11, wherein ~~an~~ each intermediate and the last encryption module~~, different from the first module, starts~~ begins encryption operations as soon as said module receives a part of the results of encryption operations from the immediately preceding encryption module.

14. (currently amended) ~~M~~A method according to Claim 11, wherein the method is carried out by three modules wherein the central module operates with a secret symmetric key.

15. (currently amended) ~~M~~A method according to claim 14, wherein the first module and the last module in respect of encryption and in reversed order the last module and the first module in respect of decryption operate with an algorithm using asymmetric keys including a private key and a public key.

16. (previously presented) ~~M~~A method according to claim 15, wherein the first module and the last module use the private key for encryption and the public key for decryption.

17. (currently amended) ~~M~~A method according to claim 16, wherein the first module and the last module use the same set of private and public keys.

18. (currently amended) ~~M~~A method according to Claim 16, wherein the first module and the last module use a different set of private and public keys.

19. (currently amended) ~~M~~A method according to Claim 15, wherein, the last module uses the public key during encryption and the first module uses the private key during decryption.

20. (currently amended) ~~M~~A method according to Claim 11, wherein the method is carried out by three encryption/decryption modules, wherein all three modules operate with asymmetric keys.

21. (New) A method of improving the security of an encryption/decryption process carried out by a plurality of decryption modules arranged in series, said method comprising the steps of:

providing from a first and each intermediate encryption/decryption module partial results of an encryption/encryption operation to each intermediate and last encryption/decryption module, respectively;

beginning, at each intermediate and last encryption/decryption module, encryption/decryption operations on said partially available result of an immediately preceding encryption/decryption module, before said immediately preceding encryption/decryption module has terminated its encryption/decryption operation;

using asymmetric keys in the encryption/decryption process in at least one of said encryption/decryption modules, wherein said asymmetric keys including a private key and a public key.

22. (New) A method according to claim 21, wherein said each intermediate and the last decryption module begins decryption operations upon receiving said partially available result from decryption operations of said immediately preceding decryption module.

23. (New) A method according to claim 21, wherein each intermediate and the last encryption module begins encryption operations upon receiving said partially available result from encryption operations of said immediately preceding encryption module .

24. (New) A method according to claim 21, wherein said series has three modules; further comprising the step of:

using a secret symmetric key in the encoding/decoding operations carried out by a central module.

25. (New) A method according to claim 24, wherein the first module and the last module in respect of encryption and in reversed order the last module and the first module in respect of decryption operate with an algorithm using asymmetric keys, wherein said asymmetric keys include a private key and a public key.

26. (New) A method according to claim 25, wherein the first module and the last module use said private key for encryption and said public key for decryption.

27. (New) A method according to claim 26, wherein the first module and the last module use the same set of private and public keys.

28. (New) A method according to claim 26, wherein the set of private and public keys used by said first module and said last module are different.

29. (New) A method according to claim 25, wherein, the last module uses the public key during encryption and the first module uses the private key during decryption.

30. (New) A method according to claim 21, wherein the series comprises three encryption/decryption modules, further comprising the step of

using asymmetric keys in the encoding/decoding process of each of said three encryption/decryption modules.